OK TO ENTER: /L.L./

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicants: Karthik Kaleedhass et al.	Confirmation No.: 3830
U.S. Patent Application No 10/581,496	Art Unit: 2436
Filed: June 27, 2007	Examiner: Lisa C. Lewis
Title: Method and System to Electronically Identify and Verify an Individual Presenting Himself for Such Identification and Verification	Attorney Docket No.: KASS-006-US

AMENDMENT AFTER FINAL

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

January 28, 2011

Dear Sir:

In response to the Office Action mailed November 29, 2010, please amend the following:

Amendments to the Claims begin on page 2.

Remarks follow the above-mentioned amendments.

The following list of claims replaces any prior listing of claims:

1. (currently amended) A method of electronically identifying and verifying an individual ~~utilising~~ utilizing at least one biometric feature of the individual including the steps of:

enrolling an individual into a database including:

(a) inputting required particulars of the individual into the database and ascertaining the existence or otherwise of the particulars of the individual in the database;

(b) capturing the biometric features of the individual wherein key features of the biometric raw data are extracted;

(c) encrypting in a dynamic manner the biometric features, the method of encryption selected based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth; and

(d) transmitting the encrypted data of the biometric features to the server and storing the encrypted data in relation to the particulars of the individual obtained in step (a) above;

verifying an individual in the database including:

(i) activating an access apparatus with a means to capture at least one biometric feature of an individual in a secure manner using dynamic encryption;

(ii) capturing the at least one biometric feature of an individual wherein key features of biometric raw data are extracted;

(iii) encrypting in a dynamic manner the at least one biometric ~~features~~ feature, a method of encryption selected based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth;

(iv) transmitting the encrypted data of the at least one biometric feature to at least one server in the access apparatus or to at least one server spatially separated from the access apparatus, wherein in a first attempt the access apparatus will attempt to send the encrypted data to the spatially separated server and upon detecting a failure in the first attempt, the access apparatus will in a second attempt send the encrypted data to any other designated server in a network, wherein the designated servers are either servers spatially separated from the access apparatus or the servers in the access apparatus; and

(v) verifying the at least one biometric feature captured in step (i) with a pre-stored biometric feature in the server in step (iv)[[.]]

wherein at least one spatially separated server is located outside the country and wherein upon positive identification and verification of the individual access is given to an auxiliary means including access to secured doors, database, computer network and servers.

2. (original) A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the server is either spatially separated from the access apparatus or is contained within the access apparatus.

3-7. (canceled).

8. (previously presented) A method of electronically identifying and verifying an individual as claimed in claim 1, wherein particulars in step (a) includes alpha-numeral data, and/or images and/or binary data wherein the binary data includes any representation capable of being stored in a binary form.

9. (canceled).

10. (previously presented) A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the server is provided in a storage medium or other device capable of recording data.

11. (original) A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the identification of the individual is executed by comparing the biometric features of the individual captured in step (ii) of claim 1 with known biometric features of the individual previously captured and stored in a database and picked out from the database by the use of a unique personal identification number (PIN) allocated to the individual and to the records in the database.

12. (original) A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the identification of the individual is executed by comparing the biometric features of the individual captured in step (ii) of claim 1 with known biometric features of the individual previously captured and stored in the database without the use of any PIN numbers.

13. (original) A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the biometric features of the individual to be identified and verified are stored in a server instead of in any storage medium held in possession by or issued to individual.

14. (original) A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the encrypted biometric features of the individual are processed by an biometric server software located at the server instead of at the point where the biometric features of an individual presenting for identification and verification are captured.

15. (previously presented) An electronic means of identifying and verifying an individual presenting for such identification and verification including:

(i) a means to capture at least one type of biometric features of the individual;

(ii) a software means to encrypt in a dynamic manner the biometric features captured in (i), a method of encryption selected based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth;

(iii) a transmission means wherein the encrypted biometric features of the individual are transmitted to a server;

(iv) a software means to capture the encrypted biometric features presented for identification and verification against stored encrypted biometric features of a purported individual; and

(v) a means to give access to other database or software if a positive identification and verification is made and to deny such access if a negative identification and verification is made.

16. (original) An electronic means of identifying and verifying an individual as claimed in claim 15 wherein identifying the individual comprises of:

a PIN number for each stored encrypted biometric features of an individual; and a means to access the stored encrypted biometric features of an individual by the provision of a correct PIN number by an individual presenting for identification and verification and a means to compare the captured biometric features of the individual with a given PIN number with the stored biometric features of the purported individual.

17. (original) A method of electronically identifying and verifying an individual as claimed in claim 1 wherein the biometric features include finger print, retina scan, iris scan or any other unique biometric features capable of being captured by sensors.

18. (previously presented) An electronic means of identifying and verifying an individual as claimed in claim 15 wherein the biometric features include~~s~~ finger print, retina scan, iris scan or any other unique biometric feature capable of being captured by sensors.

19. (previously presented) An electronic means of identifying and verifying an individual presenting for such identification and verification including:

(i) access apparatus with a means to capture at least one biometric raw data of an individual in a secure manner using dynamic encryption;

(ii) circuitry to extract any features of the biometric raw data from the means to capture the biometric raw data;

(iii) circuitry to encrypt the key features of the biometric raw data in a dynamic manner, a method of encryption selected based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth;

(iv) transmission means to transmit encrypted data of the biometric features to at least one server;

(v) at least one server to receive and store the encrypted data of the biometric feature of the individual; and

(vi) circuitry to verify and/or identify the encrypted data against pre-stored encrypted biometric data in the server.

20. (original) An electronic means of identifying and verifying an individual as claimed in claim 19 wherein the server is either spatially separated from the access apparatus or is contained within the access apparatus.

21. (original) An electronic means of identifying and verifying an individual as claimed in claim 19 includes circuitry of transmission of encrypted biometric data to a pre-designated server fails, the encrypted biometric data is routable to at least one other designated server in an pre-designated sequence.

22. (previously presented) An electronic means of identifying and verifying an individual as claimed in claim 19, wherein a token encoding data unique to the individual presenting for identification and verification has to be introduced into the access apparatus before the biometric feature of the individual is captured.

23. (previously presented) An electronic means of identifying and verifying an individual as claimed in claim 19, wherein the biometric data of an individual is stored in a encrypted manner in server and in any tokens if used.

24. (previously presented) An electronic means of identifying and verifying an individual as claimed in claim 19, wherein the means requires the introduction of a personal identification number (PIN) of an individual presenting for identification and verification into the access apparatus.

REMARKS

Favorable reconsideration of this application, in light of the following discussion, is respectfully requested. Claims 1-6 and 8-24 are pending in the present application. Claim 1 is amended by way of the present response. Claims 3-6 and 9 are canceled without prejudice or disclaimer. Applicants submit that upon entry of the present Response, claims 1-2, 8, and 10-24 are in condition for allowance. Moreover, the Applicants submit that no new matter has been introduced by the foregoing amendments.

Rejections under 35 U.S.C. § 103

In the outstanding Action, claims 1-4, 8, 10-20, 23 and 24 stand rejected under 35 U.S.C. §103(a) as allegedly unpatentable over Uchida (U.S. Patent No. 7,246,243) in view of Lindo et al. (U.S. Pub. No. 2002/0099858).

In addition, claims 5, 6 and 21 stand rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Uchida in view of Lindo and further in view of Bianco et al. (U.S. Patent No. 6,256,737).

In addition, claim 9 stands rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Uchida in view of Lindo and further in view of McCabe (U.S. Pub. No. 2002/0095317).

Finally, claim 22 stands rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over Uchida in view of Lindo and further in view of Robinson et al. (U.S. Pub. No. 2008/0271116).

Applicants respectfully traverse each of these rejections for at least the following reasons.

Independent claims 1, 15 and 19 are the independent claims presently under consideration. None of the cited references, considered alone or in combination, teach or suggest every element recited in independent claims 1, 15 and 19.

The rejection of claims 1-4, 8 10-20, 23 and 24 under 35 U.S.C. § 103(a), as allegedly unpatentable over Uchida in view of Lindo is respectfully traversed.

Amended claim 1 recites:

> A method of electronically identifying and verifying an individual utilizing at least one biometric feature of the individual including the steps of: enrolling an individual into a database including: (a)inputting required particulars of the individual into the database and ascertaining the existence or otherwise of the particulars of the individual in the database; (b)capturing the biometric features of the individual wherein key features of the biometric raw data are extracted; (c) encrypting in a dynamic manner the biometric features, the method of encryption selected based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth; and (d) transmitting the encrypted data of the biometric features to the server and storing the encrypted data in relation to the particulars of the individual obtained in step (a) above; verifying an individual in the database including: (i) activating an access apparatus with a means to capture at least one biometric feature of an individual in a secure manner using dynamic encryption; (ii) capturing the at least one biometric feature of an individual wherein key features of biometric raw data are extracted; (iii) encrypting in a dynamic manner the at least one biometric feature, a method of encryption selected based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth; (iv) transmitting the encrypted data of the at least one biometric feature to at least one server in the access apparatus or to at least one server spatially separated from the access apparatus, wherein in a first attempt the access apparatus will attempt to send the encrypted data to the spatially separated server and upon detecting a failure in the first attempt, the access apparatus will in a second attempt send the encrypted data to any other designated server in a network, wherein the

> designated servers are either servers spatially separated from the access apparatus or the servers in the access apparatus; and (v) verifying the at least one biometric feature captured in step (i) with a pre-stored biometric feature in the server in step (iv); wherein at least one spatially separated server is located outside the country and wherein upon positive identification and verification of the individual access is given to an auxiliary means including access to secured doors, database, computer network and servers.

Uchida, considered alone or in combination, does not teach or suggest each and every limitation of claim 1. Rather, Uchida discloses an identification system and method for authenticating user transaction requests from end terminals, including user terminals 10 with a fingerprint sensor 11, a fingerprint feature extraction unit 12 and an encryption unit 13. A user's fingerprint is detected by sensor 11 and a feature is extracted by extraction unit 12 and ciphered by the encryption unit 13 and forwarded to an authentication server 40 having a database for storing data. A determination is then made whether the received information has a corresponding match in the database.

Notably, and as the Examiner points out in the Response to Arguments of the most recent Office Action, Uchida does not expressly teach or suggest encrypting in a dynamic manner the biometric features or that this step is performed prior to a user inputting biometric feature information for authorization. Further, Uchida does not disclose that a method of encryption selected is based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth, as recited in the present invention.

The Examiner states that despite the lack of disclosure in Uchida, it would be obvious to extract and encrypt the features for basic security purposes. However, claim 1

not only recites an encryption feature in general, but rather an additional method of encryption selection based on factors including computing power of both the registration and server computer, as well as network bandwidth. In other words, the present invention discloses more than simple extraction and encryption, but further selects a particular method and type of encryption based on the environment and operational issues. As a result, the present invention optimizes the encryption step to secure raw data at both the identification and verification stages from tampering.

Lindo does not make up for the deficiencies of Uchida. To the contrary, Lindo merely discloses a network communications protocol including a message handler layer 2, a channel layer 4 and a socket layer 6. The Examiner appears to rely on Lindo as disclosing that a method of encryption selected is based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth. The Examiner alleges Lindo discloses that encryption operation may be selected by the user and may be defaulted depending on the available bandwidth. (See Office Action 11/29/2010, paragraph 8).

However, the method of encryption selection of the present invention requires consideration of not only available bandwidth, but also the computing power of the registration computer and the computing power of a server computer. Bandwidth is just one of three factors, and Lindo is silent at least with respect to the other claimed factors.

In addition, Applicants have amended independent claim 1 to recite further limitations with respect to transmitting the encrypted data of the at least one biometric feature to at least one server in the access apparatus or to at least one server spatially separated from the access apparatus, wherein in a first attempt the access apparatus will

attempt to send the encrypted data to the spatially separated server and upon detecting a failure in the first attempt, the access apparatus will in a second attempt send the encrypted data to any other designated server in a network, wherein the designated servers are either servers spatially separated from the access apparatus or the servers in the access apparatus. Furthermore, Applicants have amended claim 1 to recite wherein at least one spatially separated server is located outside the country. As the Examiner points out, neither Uchida nor Lindo teach these limitations (See Office Action 11/29/2010, paragraphs 26 and 32).

As such, Uchida and Lindo, alone or in combination, do not describe or suggest every element recited in claim 1. For at least the reasons set forth above, Applicants respectfully submit that independent claim 1 is patentable over Uchida and Lindo. Since dependent claims 2, 8, and 10-14 depend directly or indirectly from independent claim 1, Applicants respectfully submit that claims 2, 8, and 10-14 likewise are patentable over Uchida.

Further, independent claims 15 and 19 recite the same or similar limitations as independent claim 1. As a result, Applicants respectfully submit that claims 15 and 19 are likewise patentable over Uchida and Lindo. Since dependent claims 16-18 dependent from claim 15, and dependent claims 20 and 23-24 depend from claim 19, Applicants respectfully submit that claims 16-18, 20, and 23-24 likewise are patentable over Uchida and Lindo.

With respect to the rejections of claims 5, 6, and 21 under 35 U.S.C. § 103(a) as allegedly unpatentable over Uchida in view of Lindo and further in view of Bianco, Applicants respectfully traverse.

As noted, claims 5 and 6 are canceled without prejudice or disclaimer. Applicants respectfully submit that these rejections are now moot. However, aspects of claims 5 and 6 are now incorporated into independent claim 1, and in the interest of promoting the prosecution of the present invention, Applicants will address the rejections herein.

As discussed above, Uchida and Lindo do not teach or suggest every element recited in claims 1, 15 and 19. Bianco does not make up for the deficiencies of Uchida and Lindo.

Rather, Bianco merely discloses a system, method and computer program product for allowing access to enterprise resources using biometric devices. The system includes a biometric server storing collections of data to authenticate users. Like Uchida, Bianco mentions encryption as a means of providing security to a system, but does not teach, suggest or disclose selecting a method and type of encryption. Further, like Uchida and Lindo, Bianco is silent regarding a method of encryption selected based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth, as described by the present invention.

As a result, none of Uchida, Lindo or Bianco, considered alone or in combination, teach, suggest, or disclose each and every limitation of independent claims 1, 15, and 19. For at least the reasons set forth above, Applicants respectfully submit that independent claims 1, 15, and 19 are patentable over Uchida, Lindo and Bianco. Since dependent claim 21 depends from claim 19, Applicants respectfully submit that claim 21 likewise is patentable over Uchida, Lindo and Bianco.

With respect to the rejection of claim 9 as allegedly unpatentable over Uchida in view of Lindo and further in view of McCabe, Applicants respectfully traverse.

As noted, claim 9 is canceled without prejudice or disclaimer. Applicants respectfully submit that this rejection is now moot. However, aspects of claim 9 are now incorporated into independent claim 1, and in the interest of promoting the prosecution of the present invention, Applicants will address the rejection herein.

As discussed above, Uchida and Lindo do not teach or suggest every element recited in claims 1, 15, and 19. McCabe does not make up for the deficiencies of Uchida and Lindo.

Rather, McCabe merely discloses a data/presence insurance tools and technique. McCabe appears altogether unrelated to the present invention, and certainly makes no mention of selecting a method and type of encryption or a method of encryption selected based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth, as described by the present invention.

As a result, none of Uchida, Lindo, or McCabe, considered alone or in combination, teach, suggest, or disclose each and every limitation of independent claims 1, 15, and 19. For at least the reasons set forth above, Applicants respectfully submit that independent claims 1, 15, and 19 are patentable over Uchida, Lindo, and McCabe.

With respect to the rejection of claim 22 as allegedly unpatentable over Uchida in view of Lindo and further in view of Robinson, Applicants respectfully traverse.

As discussed above, Uchida and Lindo do not teach or suggest every element recited in claims 1, 15, and 19. Robinson does not make up for the deficiencies of Uchida and Lindo.

Rather, Robinson discloses a system and method of enrolling potential system users for a biometric system for identity verification. Robinson only discloses that information transferred between two points in the system is encrypted, but does not teach suggest or disclose selecting a method and type of encryption or a method of encryption selected based on factors including the computing power of a registration computer, the computing power of a server computer, and network bandwidth, as described by the present invention.

As a result, none of Uchida, Lindo, or Robinson, considered alone or in combination, teach, suggest, or disclose each and every limitation of independent claims 1, 15, and 19. For at least the reasons set forth above, Applicants respectfully submit that independent claims 1, 15, and 19 are patentable over Uchida, Lindo, and Robinson. Since dependent claim 22 depends from claim 19, Applicants respectfully submit that claim 22 likewise is patentable over Uchida, Lindo, and Robinson.

Accordingly, for at least the reason set forth above, Applicants respectfully request that the §103 rejections be withdrawn.

CONCLUSION

Consequently, in view of the present amendment and in light of the above discussion, the outstanding grounds of rejection are believed to have been overcome. The application, as amended, is believed to be in condition of allowance. An early and favorable action to that effect is respectfully requested.

Respectfully submitted,

/Timothy J. Maier/
Timothy J. Maier
Attorney of Record
Reg. No. 51,986

Maier & Maier, PLLC
1000 Duke Street
Alexandria, VA 22314
Customer No. 62008
January 28, 2011